DE4843J1-1（第1版）897E 35420

富士ゼロックス Print Server N01
セキュリティー対策に関する補足情報

2011 年 7 月　第 1 版

このたびは、Print Server N01 をご利用いただき、まことにありがとうございます。

本書では、Print Server を運用する際の、セキュリティー対策に関する情報を説明しています。
Print Server をご利用になる前に、『Print Server N01 ユーザーズガイド導入編』、『Print Server N01 ユーザーズガイド運用編』、および『Print Server N01 Ver.6.0 リリースについての追加補足情報』とあわせて、ここで説明している情報をお読みください。

◆ 本製品は、オペレーティングシステムとして、マイクロソフト株式会社の Windows 7 を使用しています。

◆ 設置後に本製品を運用するにあたり、ウィルスなどに感染するおそれがあります。
設置後のセキュリティー対策は、本製品をご使用になるお客様が実施してください。
セキュリティー対策の情報などについては、マイクロソフト社から都度案内されます。
2011 年 6 月 15 日時点では、次の URL にアクセスすると、セキュリティー対策の情報を参照できます。
なお、次の URL は変更される場合があるため、最新の URL で確認してください。

- セキュリティー対策全般に関する情報
  - マイクロソフト株式会社　http://www.microsoft.com/japan/security/default.mspx
  - 株式会社シマンテック　http://www.symantec.com/ja/jp/index.jsp
  - マカフィー株式会社　http://www.mcafee.com/japan/security/
- 本製品に関する情報
  - 富士ゼロックス株式会社　http://www.fujixerox.co.jp/

◆ 本製品では、Windows 7 と 2011 年 6 月 15 日現在までにリリースされたセキュリティーパッチのうち、本製品に関連するセキュリティーパッチを導入しています。

◆ 株式会社シマンテックの「Symantec Endpoint Protection 11.0」、マカフィー株式会社の「McAfee VirusScan Enterprise 8.7」については、Print Server での動作を確認済みです。ただし、これらのソフトウエアに欠陥がないことを保証するものではありません。

◆ ウィルス対策のソフトウエアを使用すると、Print Server の動作が遅くなる場合があります。

◆ Print Server ではセキュリティ対策のため、NetBIOS over TCP/IP ポートや AFP over TCP/IP ポートは閉じた状態となっています。そのため、以下の機能はデフォルト設定では使用できません。

- Windows ネットワーク共有プリンタ
- ホットフォルダの Windows ネットワーク共有および AFP over TCP 共有
- TIFF フォルダの Windows ネットワーク共有および AFP over TCP 共有

上記の機能を使用する場合は、DVD内の「¥Server¥etc¥RRAS_setup」フォルダーにある「README.pdf」の内容に従って設定を変更してください。

◆ ウィルススキャンは、Fuji Xerox Print Server Service を停止したあとに手動で行ってください。

◆ セキュリティーパッチを適用する場合、またはウィルス対策（McAfee など）をインストールする場合は、ServerManager を終了してから行ってください。ServerManager を起動したまま行った場合、ServerManager のレイアウトが変わってしまうことがあります。このような場合は、ServerManager の [表示] → [標準に戻す] を選択したあとに、ServerManager をいったん終了し、再起動してください。
また、セキュリティーパッチを適用した場合は、Print Server を再起動してください。

◆ 株式会社シマンテックの「Symantec Endpoint Protection」をインストールすると、ファイアウォール機能により、一部の機能が正しく動作しない場合があります。この場合は、ファイアウォールルールで、以下の設定が必要です。

・ Mac OS X クライアントで、［システム環境設定］→［プリントとファクス］を選択して表示される［プリントとファクス］ダイアログボックスで、Print Server が表示されない場合は、AppleTalk（0x809B）、および AppleTalk（0x80F3）の接続ポートを許可してください。

・ Windows クライアントの場合（ServerManager の［システム］→［初期設定］→［サーバーの通信設定］の設定がデフォルトのとき）は、TCP/IP のリモートポート（50000）、およびローカルポート（50000）を許可してください。

◆ ウィルスバスター 2011 をインストールしていると、リアルタイムスキャン機能を停止しても、自動的に開始されることがあります。